

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)



REC'D 24 FEB 1999
WIPO PCT

Bescheinigung

09/402322

Die Deutsche Telekom AG in Bonn/Deutschland hat eine
Patentanmeldung unter der Bezeichnung

"Verfahren und Anordnung zur Erzeugung binärer
Sequenzen von Zufallszahlen"

am 2. Februar 1998 beim Deutschen Patentamt eingereicht.

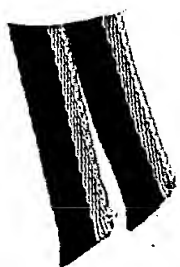
Die angehefteten Stücke sind eine richtige und genaue Wieder-
gabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patentamt vorläufig die Sym-
bole G 07 C, G 01 J und H 04 L der Internationalen Patent-
klassifikation erhalten.

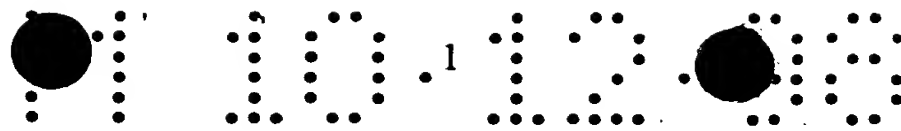
München, den 12. Oktober 1998
Der Präsident des Deutschen Patentamts
Im Auftrag

Aktenzeichen: 198 06 178.1

Ebert



BEST AVAILABLE COPY

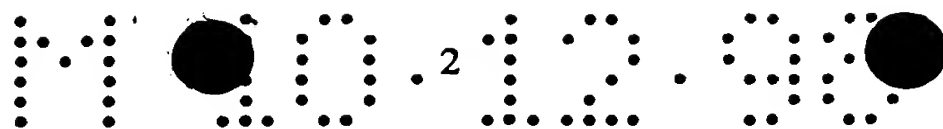


P 97185

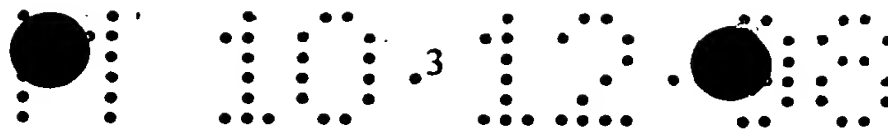
Verfahren und Anordnung zur Erzeugung binärer Sequenzen von Zufallszahlen

5 (10) Patentansprüche

1. Verfahren zur Erzeugung binärer Sequenzen von Zufallszahlen, welches auf dem Prinzip der zufälligen Wegwahl von Photonen an einem Strahlteiler und der Generierung einer Zufallszahl mittels zwei einem Strahlteiler nachgeordneten Detektoren beruht, und bei dem die Zählelektroniken der beiden Detektoren so geschaltet sind, daß eine Zufallszahl dann generiert wird, wenn nur einer der Detektoren anspricht, **d a d u r c h g e k e n n z e i c h n e t**,
daß die von einer als Lichtquelle (L) geringer Leistung ausgebildeten Photonenquelle entsprechend dem Zufallsprinzip während einer vorgegebenen Meßzeit emittierten Photonen/Photonenschwärme durch mindestens zwei nacheinander im Strahlgang der Lichtquelle (L) angeordnete Strahlteiler (ST1;ST2) aufgeteilt und entsprechend der Aufteilung über die den Strahlteilern (ST1;ST2) nachgeordneten, mit der Erfassungseinrichtung (E) verbundenen Detektoren (DT;D1₀,D2₁) erfaßt werden, und daß eine Zufallszahl nur erzeugt wird, wenn die an den einzelnen Detektoren (DT;D1₀,D2₁) registrierten Photonen in ihrer Gesamtheit einem vorher festgelegten Photonenschema entsprechen.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß bei zwei nacheinander im Strahlgang der Lichtquelle (L) angeordneten Strahlteilern (ST1;ST2) das der Erzeugung der Zufallszahl zugrunde liegende Photonenzahlschema darauf beruht, daß eine Zufallszahl nur erzeugt wird, wenn während der vorgegebenen Meßzeit am Triggerdetektor (DT) des ersten Strahlteilers (ST1) kein Photon und nur an einem der dem zweiten Strahlteiler (ST2) nachgeordneten Detektoren (D1₀) bzw. (D2₁) mindestens ein Photon registriert wird.



3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß bei zwei nacheinander im Strahlgang der Lichtquelle angeordneten Strahlteilern (ST1;ST2) das der Erzeugung der Zufallszahl zugrunde liegende Photonenzahlschema darauf beruht, daß eine Zufallszahl nur erzeugt wird, wenn während der vorgegebenen Meßzeit am Detektor (DT) des ersten Strahlteilers (ST1) mindestens ein Photon und nur an einem der dem zweiten Strahlteiler (ST2) nachgeordneten zwei Detektoren (D1₀) bzw. (D2₁) mindestens ein Photon registriert wird.
4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß für den Fall, daß mehr als zwei Triggerstrahlteiler im Strahlgang zwischen der Lichtquelle (L) und dem Strahlteiler (ST2) angeordnet sind, das Photonenschema mathematisch so ausgebildet ist, daß eine Zufallszahl nur erzeugt wird, wenn ein Photonenschwarm mit einer durch das vorgegebene Photonenschema definierten Anzahl von Photonen an den Detektoren des Strahlteilers (ST2) und den Triggerdetektoren der zusätzlichen Triggerstrahlteiler auftritt.
5. Anordnung zur Erzeugung binärer Sequenzen von Zufallszahlen, umfassend
- eine als Photonenquelle ausgebildete Lichtquelle,
 - einen der Lichtquelle nachgeordneten Strahlteiler mit zwei dem Strahlteiler nachgeordneten Detektoren und
 - eine den Detektoren nachgeordnete, aus Zähler und Rechner bestehende Erfassungseinrichtung zur Generierung der Zufallszahlen,
- d a d u r c h g e k e n n z e i c h n e t**, daß als Photonenquelle eine Lichtquelle (L) geringer Leistung eingesetzt wird, aus der entsprechend dem Zufallsprinzip sowohl einzelne Photonen als auch Photonenschwärme austreten können, und daß zwischen der Lichtquelle (L) und dem im Strahlgang der Lichtquelle (L) angeordnetem Strahlteiler (ST2) mindestens ein weiterer Strahlteiler, vorzugsweise ein Triggerstrahlteiler (ST1), im Strahlgang angeordnet ist, welcher über einen Detektor, vorzugsweise einen Triggerdetektor (DT), mit der Erfassungseinrichtung (E) verbunden ist.



6. Anordnung nach Anspruch 5, dadurch gekennzeichnet, daß als Lichtquelle (L) ein abgeschwächter Laser verwendet wird.

5 7. Anordnung nach Anspruch 5, dadurch gekennzeichnet, daß als Lichtquelle (L) eine thermische Lichtquelle verwendet wird.

8. Anordnung nach Anspruch 5, dadurch gekennzeichnet, daß als Lichtquelle (L) eine Spektrallampe verwendet wird.

10 9. Anordnung nach Anspruch 5, dadurch gekennzeichnet, daß als Lichtquelle (L) eine Leuchtdiode verwendet wird.

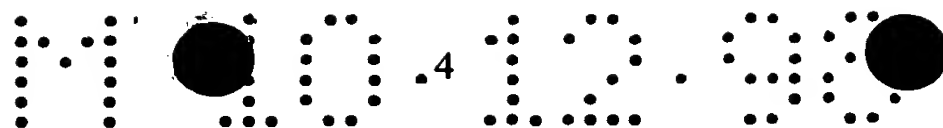
10. Anordnung nach Anspruch 4, dadurch gekennzeichnet, daß als Lichtquelle (L) eine Quetschlichtquelle verwendet wird.

15

20

25

30



P 97185

Verfahren und Anordnung zur Erzeugung binärer Sequenzen von Zufallszahlen

5 Beschreibung:

Die Erfindung betrifft ein Verfahren und eine Anordnung zur Erzeugung binärer Sequenzen von Zufallszahlen.

10 Zufallszahlen werden bei der mathematischen Simulation zufälliger Prozesse, bei der Stichprobenerhebung und besonders in der Kryptologie verwendet. Durch die zunehmend hochbitratige, digitale Kommunikation über öffentlich zugängliche Nachrichtenkanäle ist die Gewährleistung der Geheimhaltung und der Authentizität der übertragenen Information zu einem zentralen Problem geworden. Gute kryptographische Schlüssel sind Sequenzen von binären Zufallszahlen. Zur sicheren Verschlüsselung wird
15 vorzugsweise ein zufälliger Schlüssel dieser Art gewählt, der so lang wie die Nachricht selbst ist und nur ein einziges Mal Verwendung findet.

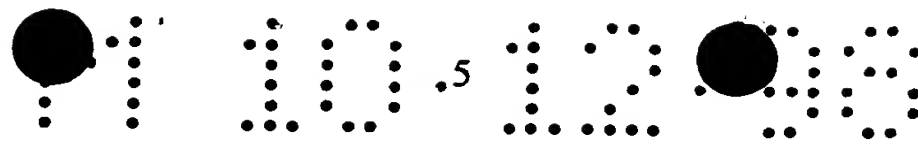
Zur Erzeugung von Zufallszahlen stehen im Wesentlichen zwei verschiedenartige Möglichkeiten zur Verfügung:

20 1. durch mathematische Algorithmen generierte Pseudo-Zufallszahlen

Echte Zufallszahlen lassen sich in einem Rechner, der ja vollständig deterministisch arbeitet, grundsätzlich nicht erzeugen. Die durch mathematische Algorithmen generierten Zufallszahlen, die viele Programme zur Verfügung stellen, sind daher nie wirklich zufällig. Eine Verbesserung stellen die sogenannten Pseudozufallszahlen dar, die aus einem
25 kürzeren echt zufälligen Keim entwickelt werden.

In jedem Fall ist jedoch bei der Generierung von Pseudozufallszahlen nach den o.g. Verfahrenswegen mit einer gewissen Anzahl, von vorne herein unbrauchbarer Sequenzen (schwache Schlüssel) und auf jeden Fall mit seltsamen Korrelationen zu rechnen.

30 2. Zufallszahlen, die auf physikalischen Verfahren basieren



Bei diesen Verfahren wird der statistische Charakter bestimmter physikalischer Prozesse genutzt.

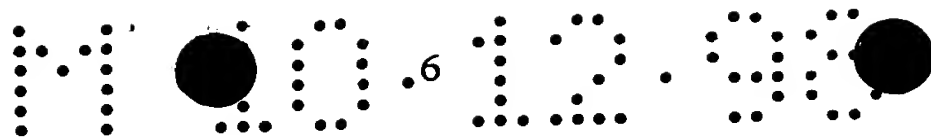
Auch bei den physikalischen Verfahren gibt es solche, die zwar im Grunde deterministisch, aber dabei so komplex sind, daß sie nicht reproduziert werden können. Dazu gehören etwa der Münzwurf "Kopf" oder "Zahl", oder die Lottomaschinen. Diese Verfahren produzieren ein deterministisches Chaos, das als zufällig gelten kann, da die Anfangsbedingungen des Generators bei der Erzeugung jeder einzelnen Zufallszahl stets etwas voneinander abweichen, ohne daß diese Abweichung quantifizierbar wird.

Zu den physikalischen Verfahren gehören auch Elementarprozesse wie sie beispielsweise in der Quantenmechanik vorkommen. Derartige Prozesse sind von ihrer Natur her grundsätzlich zufällig. Zufallszahlen, die durch physikalische Prozesse erzeugt werden, kommen daher dem Konzept einer zufälligen Sequenz näher als algorithmisch generierte Zufallszahlen.

Bekannt ist eine Lösung, die den natürlichen Quantenprozeß des elektromagnetischen Rauschens eines Widerstandes oder einer Diode zur Erzeugung von zufälligen Bitsequenzen nutzt (siehe Manfred Richter: Ein Rauschgenerator zur Gewinnung von quasii-dealen Zufallszahlen für die stochastische Simulation, Dissertation RWTH Aachen ; 1992).

Derartige Verfahren können jedoch von außen dadurch manipuliert werden, daß dem Quantenrauschen ein willkürlich vorgegebenes "Rauschen" etwa durch Einstrahlung elektromagnetischer Wellen überlagert wird. Da die Trennung des Quantenrauschens von diesem fremdbestimmten Pseudoruschen nicht einfach ist, gelten derartige Verfahren als nicht sicher.

Desweiteren sind Verfahren zur Generierung von Zufallszahlen bekannt, die auf radioaktiven Zerfallsprozessen basieren (siehe Martin Gude: „Ein quasi-idealer Gleichverteilungsgenerator basierend auf physikalischen Zufallsphänomenen“;Dissertation RWTH Aachen 1987). Dieses Verfahren eignet sich aufgrund der hohen Energie der entstehenden Teilchen sehr gut um Zufallssequenzen zu erzeugen, allerdings bestehen neben den wirklich vorhandenen Gefahren, die insbesondere auf der potentiell schädlichen Wirkung



radioaktiver Strahlung auf den Menschen beruhen, bei einem Teil der Bevölkerung irrationale Vorbehalte gegenüber der Radioaktivität, so daß radioaktive Prozesse nicht ohne weiteres zur Zufallserzeugung verwendet werden können.

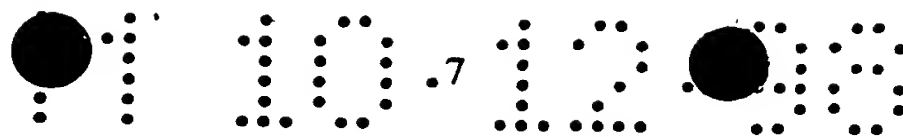
- 5 Ein weiteres bekanntes Verfahren zur Erzeugung von Zufallssequenzen basiert auf dem Prozess der Wegwahl einzelner Photonen am Strahlteiler (siehe J.G. Rarity et al.: „Quantum random-number Generation and key sharing“ ; J. Mod. Opt. 41, S.2435 1994) Bei diesem Verfahren wird ein Lichtquant z. B. an einem halbdurchlässigen Spiegel reflektiert oder transmittiert; zwei Detektoren registrieren das Lichtquant und ihre Anzeigen repräsentieren die "0" oder die "1" der Zufallssequenz.

- 10 Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren und eine Anordnung zur Erzeugung binärer Sequenzen von Zufallszahlen bereitzustellen, durch die die oben beschriebenen Nachteile vermieden werden. Die Lösung soll dabei kostengünstiger als die bekannten Lösungen sein und sich ohne großen Aufwand auf eine Chipkarte integrieren lassen.

Die Aufgabe wird erfindungsgemäß durch die kennzeichnenden Merkmale des 1. Patentanspruchs gelöst. Vorteilhafte Ausgestaltungen und Weiterbildungen ergeben sich aus den Unteransprüchen.

- 20 Die erfindungsgemäße Lösung basiert auf dem bekannten Prinzip der Wegwahl einzelner Photonen an einem Strahlteiler. Bei der erfindungsgemäßen Lösung wird ein optischer Strahlteiler, z. B. ein halbdurchlässiger Spiegel verwendet, auf den ultraviolettes, sichtbares oder infrarotes Licht fällt. Zwei Detektoren, die einzelne Photonen erkennen können, registrieren die Photonen und definieren über die ihnen zugeordneten Anzeigen die „0“ oder die „1“ der Zufallssequenz und damit die Zufallsfolge.

- 25 Bei dem erfindungsgemäßen Verfahren wird als Lichtquelle L anstatt der bisher üblichen Photonenquelle, wie beispielsweise eine abgeschwächte Laserstrahlquelle, eine Photonenquelle geringerer Leistung und damit auch geringerer Abmessung eingesetzt. Geeignet sind beispielsweise abgeschwächte Laserdioden, normale Dioden (LEDs), thermische Lichtquellen wie Halogenlampen, Spektrallampen oder Quetschlichtquellen. Desweiteren wurde erfindungsgemäß vor dem zweiten Strahlteiler ST2 ein erster Strahlteiler ST1,
- 30



vorzugsweise ein Triggerstrahlteiler, in den Strahlgang der Lichtquelle L eingefügt. Die entsprechend dem Zufallsprinzip von der Lichtquelle L während einer vorgegebenen Meßzeit emittierten Photonen/Photonenschwärme werden dabei durch die im Strahlgang der Lichtquelle L angeordneten Strahlteiler ST1 und ST2 aufgeteilt und entsprechend der Aufteilung über die den Strahlteilern ST1 und ST2 nachgeordneten Detektoren (Triggerdetektor DT für Strahlteiler ST1 und die Detektoren D1₀ und D2₁ für den Strahlteiler ST2) erfaßt.

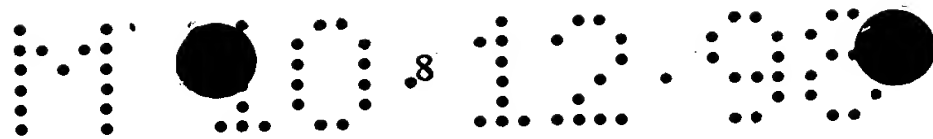
Die Detektoren DT, D1₀ und D2₁ sind mit der Erfassungseinrichtung E verbunden. Eine Zufallszahl wird nur erzeugt, wenn die an den einzelnen Detektoren DT, D1₀ und D2₁ registrierten Photonen in ihrer Gesamtheit einem vorher festgelegten Photonenzahl-schema entsprechen, welches in den Rechner der Erfassungseinrichtung eingegeben wurde.

Die mathematischen Grundlagen sowie die möglichen Ausführungsformen der erfindungsgemäßen Lösung werden nachfolgend anhand von Figur 1 näher erläutert.

Als Lichtquelle L wird eine Lichtquelle gewählt, bei der Lichtintensität derart schwach ausgebildet ist, daß sie einzelne Photonen oder aber stets mit einer gewissen Wahrscheinlichkeit auch Photonenschwärme aus n Photonen aussendet. Diese Photonenschwärme werden dann in den Detektoren DT, D1₀ und D2₁ entweder aufgelöst oder als ganzes als Einzelergebnis gezählt. Die Wahrscheinlichkeit p_n, daß am Detektor gleichzeitig n Photonen auftreten oder als Einzelereignis gezählt werden, wird durch die Poissonverteilung beschrieben.

$$p_n = \frac{\bar{n}^n}{n!} e^{-\bar{n}} \quad (1)$$

\bar{n} ist die mittlere Zahl der Photonen pro Meßzeit am Detektor. Obwohl die Statistik der Lichtquelle für thermisches Licht (Halogenlampe), chaotisches Licht (Spektrallinie) oder Laserlicht verschieden ist, gilt Gleichung (1) für alle diese Lichtquellen, solange die Kohärenzzeit einer thermischen oder chaotischen Quelle kurz im Vergleich zu Meßzeit des Detektors ist. Für Laserlicht gilt immer die Gleichung (1). Beim einfachen Strahlteiler



mit zwei Detektoren, wie er durch den Strahlteiler ST2 und die Detektoren D1₀ und D2₁ in Fig. 1 abgebildet ist, wird die Elektronik der Zählvorgänge so eingerichtet, daß ein Ergebnis immer nur dann gezählt wird, wenn nur einer der Detektoren D1₀ oder D2₁ anspricht. Sprechen beide Detektoren D1₀ und D2₁ innerhalb der Meßzeit an, so wird das Zählereignis verworfen. Wird ein Schwarm von Photonen am Strahlteiler ST2 aufgeteilt, so wird das Ereignis nicht gewertet. Gewertet wird ein Zählereignis nur, wenn der Schwarm völlig in den einen Detektor D1₀ oder völlig in den anderen Detektor D2₁ gelangt und gezählt wird. Bei einem Schwarm von n Photonen bedeutet dies, daß nur 2 von n+1 Ereignissen gezählt werden, und Gleichung (1) ist daher noch mit $\frac{2}{n+1}$ zu multipli-

zieren, um die Wahrscheinlichkeit zu beschreiben, mit der Zählereignisse bei einem Photonenschwarm auftreten. Also:

Die Wahrscheinlichkeit p_n, daß bei einer mittleren Photonenzahl \bar{n} ein brauchbares Zählereignis auftritt, beträgt für den einfachen Strahlteiler, entsprechend Strahlteiler ST2, und einer der oben beschriebenen Lichtquellen L geringer Leistung

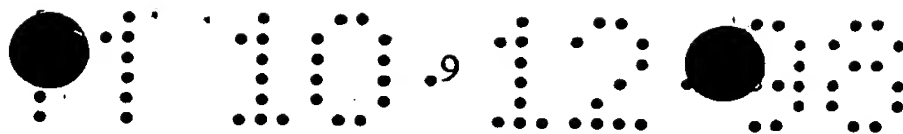
15

$$p_n^{(1)} = \frac{\bar{n}^n}{n!} e^{-\bar{n}} \cdot \frac{2}{n+1} \quad \text{einfacher Strahlteiler} \quad (2)$$

Erfindungsgemäß wird dem einfachen Strahlteiler ST2 ein weiterer Strahlteiler St1, vorzugsweise ein Triggerstrahlteiler, vorschaltet (Fig.1). Wie im ersten Fall sind die Zähl-elektroniken der beiden Detektoren D1₀ und D2₁ so geschaltet, daß eine Zufallszahl nur dann bestimmt wird, wenn nur der eine oder nur der andere Detektor D1₀ oder D2₁ anspricht. Außerdem darf in diesem Fall aber der Triggerdetektor DT des Strahlteilers ST1 nicht ansprechen. Laufzeiteffekte zwischen dem Triggerdetektor DT des ersten Strahlteilers ST1 und den Detektoren D1₀ und D2₁ des zweiten Strahlteiler ST2 werden optisch oder elektronisch ausgeglichen. Tritt ein Schwarm von n Photonen auf, und gelangt wenigsten 1 Photon des Schwarmes in den Triggerdetektor DT, wird das Ereignis nicht gezählt. Nur wenn kein Photon über den ersten Strahlteiler ST1 zum Triggerdetektor DT gelangt und außerdem am zweiten Strahlteiler ST2 alle n Photonen vollständig, entweder in den Detektor D1₀, oder in den Detektor D2₁ gelangen, wird ein Ergebnis als (0) oder (1) gezählt. Die Wahrscheinlichkeit, daß kein Photon des Schwarmes zum

30

...



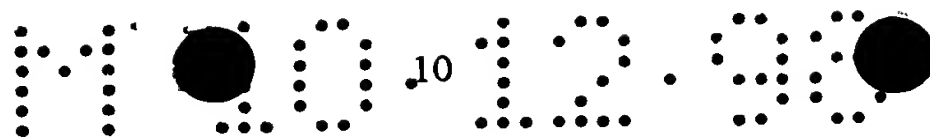
Triggerdetektor DT gelangt und der Rest völlig zu einem der Detektoren $D1_0$ oder $D2_1$, beträgt $4/((n+1)(n+2))$, d. h. die Wahrscheinlichkeit $p_n^{(2)}$, daß bei einem Schwarm von n Photonen ein Zählereignis auftritt, beträgt

$$p_n^{(2)} = \frac{\bar{n}^n}{n!} e^{-\bar{n}} \cdot \frac{4}{(n+1)(n+2)} \quad \text{Strahlteiler ST2 mit vorgeschaltetem Strahlteiler ST1} \quad (3)$$

Die Gleichung (3) gilt für den Fall, daß der Strahlteiler ST1 das Teilungsverhältnis $1/3 : 2/3$, der Strahlteiler ST2 aber das Teilungsverhältnis $1/2 : 1/2$ hat. In diesem Fall werden die drei Detektoren DT, $D1_0$, $D2_1$ gleich gewichtet. Andere Teilungsverhältnisse sind möglich, verändern aber die Wahrscheinlichkeiten nach Gleichung (3).

Das hier angewendete Verfahren macht es also mit zunehmender Anzahl n der während einer vorgegebenen Meßzeit emittierten Photonen immer unwahrscheinlicher, daß ein n -Photonenschwarm zu einem Zählereignis und damit zu einer Zufallszahl führt. Aber die Wahrscheinlichkeit nimmt zu, daß der quantenmechanisch ideale Fall eintritt: nämlich die Erzeugung des Zufalls durch ein einzelnes Photon am Strahlteiler. Die Mehrphotonenereignisse, die im Grenzfall großer n in den klassischen Zustand übergehen, werden unterdrückt. Damit können erfindungsgemäß schwache Laser, chaotische oder thermische Lichtquellen zur Zufallserzeugung herangezogen werden.

Denkbar ist auch die Anordnung von mehr als einem Triggerstrahlteiler, in den Strahlgang zwischen Lichtquelle L und Strahlteiler ST2. Die Triggerdetektoren dieser zusätzlichen Triggerstrahlteiler sind ebenfalls mit der Erfassungseinrichtung E verbunden. Bei einer derartigen Ausführungsform werden die während der vorgegeben Meßzeit detektierten Photonen, entsprechend ihrer Zuordnung zu den einzelnen Triggerstrahlteilern (einschließlich Strahlteiler ST2), in der Erfassungseinrichtung registriert und ebenfalls mit einem vorher festgelegten, in der Erfassungseinrichtung E gespeicherten Photonenschema verglichen. Bei einer solchen Ausführungsform werden Photonenschwärme noch stärker unterdrückt. Zufallseignisse werden beispielsweise nur registriert, wenn keiner der Triggerdetektoren anspricht.



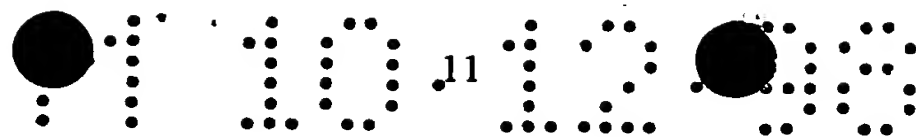
Auch ein anderes festgelegtes oder variabel veränderbares Photonenschema kann bei einer Ausführungsform mit mehreren Triggerdetektoren im Strahlgang der Lichtquelle L vorgegeben werden. Das Photonenschema kann beispielsweise beinhalten, daß der Triggerdetektor jedes zweiten Triggerstrahlteilers ansprechen muß, oder daß nur der Triggerdetektor des ersten und des siebten Triggerstrahlteilers ansprechen muß. In jedem dieser Fälle wird die Zählwahrscheinlichkeit für den Photonenschwarm vermindert.

Ein interessantes Beispiel ist eine Anordnung nach Fig. 1, bei der Zufallsereignisse am zweiten Strahlteiler ST2 nur gezählt werden, wenn ein oder mehrere Photonen durch den Triggerdetektor DT des Strahlteilers ST1 registriert werden. In diesem Fall werden Schwärme mit nur einem Photon gar nicht für die Zufallserzeugung verwendet. Da die heutigen Detektoren auch recht unangenehme Eigenschaften, wie geringe Quanteneffizienz und Totzeiten haben, handelt man sich mit weiteren zusätzlichen Triggerstrahlteilern auch zusätzliche elektronische Schwierigkeiten und Kosten ein. In der Praxis wird also vorzugsweise nur ein zusätzlicher Triggerstrahlteiler eingesetzt werden.

20

25

30



Bezugszeichenaufstellung:

L	Lichtquelle
ST1	erster Strahlteiler (Triggerstrahlteiler)
5 ST2	zweiter Strahlteiler
E	Erfassungseinrichtung
DT	Triggerdetektor des ersten Strahlteilers

D1₀ I

10 I

Detektoren des zweiten Strahlteilers

D2₁ I

n

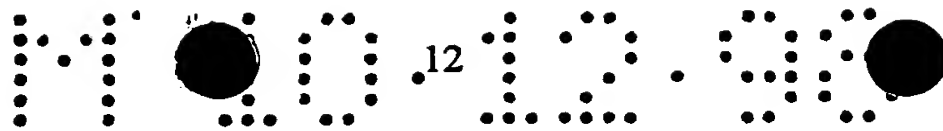
Anzahl der während einer vorgegebenen Meßzeit durch die Lichtquelle emittierten Photonen

15

20

25

30



Zusammenfassung:

1.1. Verfahren und Anordnung zur Erzeugung binärer Sequenzen von Zufallszahlen

5 **2.1.** Ziel der Erfindung ist ein kostengünstiges Verfahren und eine Anordnung zur Erzeugung binärer Sequenzen von Zufallszahlen. Die Lösung soll dabei so konzipiert werden, daß eine Integration auf eine Chipkarte in einfacher Art und Weise möglich ist.

10 **2.2.** Das erfindungsgemäße Verfahren basiert auf dem Prinzip der zufälligen Wegwahl von Photonen an einem Strahlteiler und der Generierung einer Zufallszahl mittels zwei einem Strahlteiler (ST2) nachgeordneten Detektoren ($D1_0; D2_1$). Erfindungsgemäß wird zur Erzeugung von Photonen eine Lichtquelle (L) geringer Leistung verwendet und dem Strahlteiler ST2 ein zusätzlicher Strahlteiler ST1 vorgeschaltet.

15 Die von der Lichtquelle (L) während einer vorgegebenen Meßzeit emittierten Photonen werden durch die nacheinander im Strahlengang der Lichtquelle (L) angeordnete Strahlteiler (ST1; ST2) aufgeteilt. Die Erzeugung der Zufallssequenz erfolgt bei Übereinstimmung der Aufteilung der Photonen mit einem vorher festgelegten Photonenschema.

20

2.3. Die erfindungsgemäße Lösung stellt einen kostengünstigen Zufallsgenerator zur Verfügung, der sich insbesondere aufgrund der verwendeten Lichtquelle (L) in einfacher Art und Weise auf eine Chipkarte integrieren läßt.

25 **3.0. Fig. 1**

10.12.88

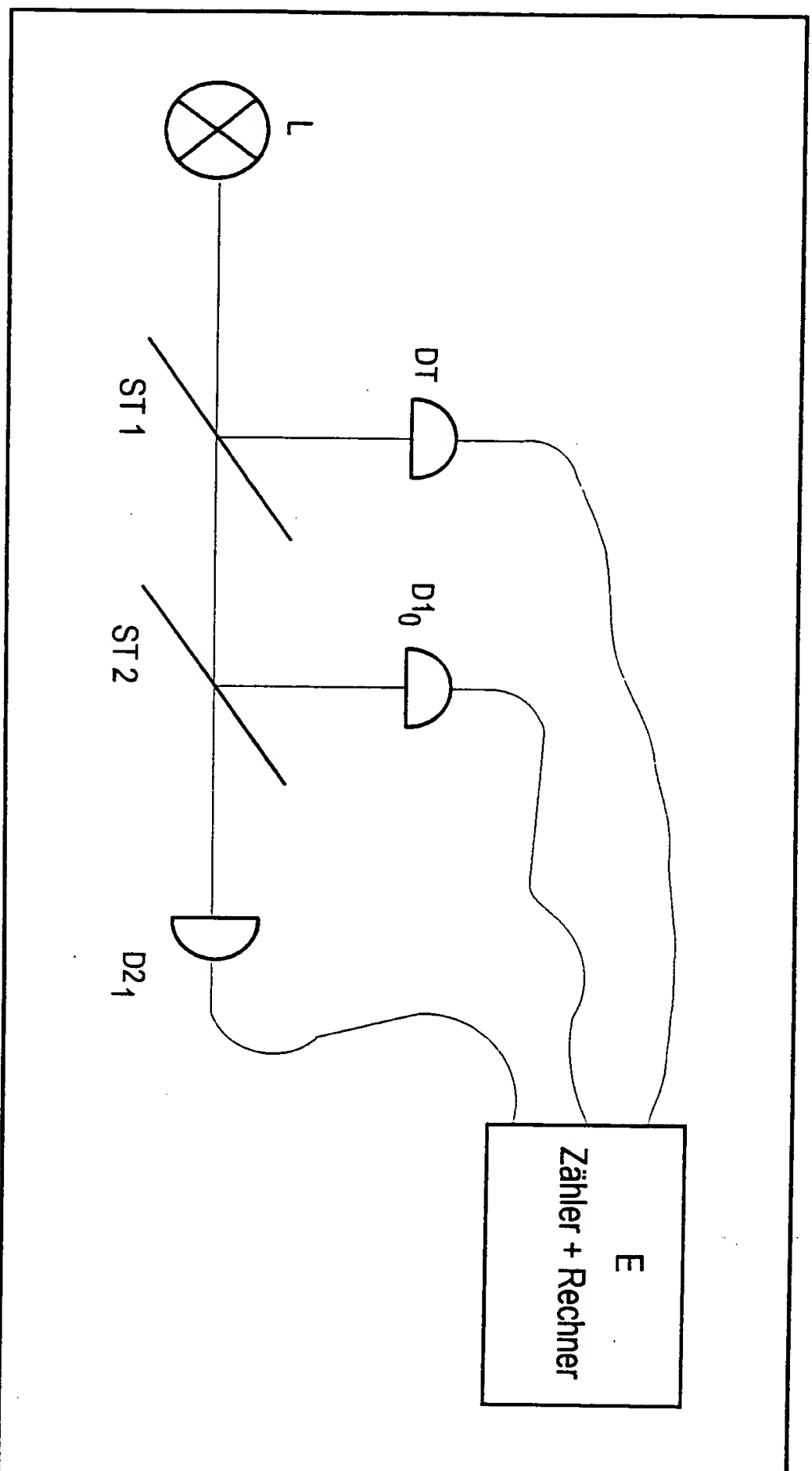


Fig. 1

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)